International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Passive Copy-Move Tamper Detection Methods for Digital Images

V.Thirunavukkarasu, M.Ranganathappa, J.SatheeshKumar

Abstract: ***Copy-move tamper discovery in digital image is a significant research application in forensic investigation. Developing an imperative and reliable means to discover copy-move tampering in order to guarantee the authenticity of digital images is a solitary research area in image processing. This category of tampering is performed to hide some unwanted information or duplicate certain region of image. This article introduces a generic algorithmic skeleton to copy-move tamper discovery Experiments are carried out on three states of art copy-move tamper detection methods with respect to three different data sets. Empirical results indicates that PCA based method is better than Frequency transformation and Zernike moment based method in terms of detection accuracy in all three data sets. This article also identified the key challenges and opportunities in copy-move tamper detection.***

Index Terms: Copy-move, forensic investigation, image processing, legitimacy, robust.

I. INTRODUCTION

Copy-move is a familiar category of image exploitation which is performed along with different kind of geometric transformations and image distortions to match the irregularities among genuine and tampered region of an image [1]. In general, tampered patterns will combine the background details of an image, thus the manual detection of this tampering is a critical task. Hence, development of competent counterfeit discovery scheme becomes a demanding task due to its higher influence. There exist different methods in literature to discover this forgery but accuracy, false positive rate, type and size of image features, robustness against different geometric operations (translation, rotation, scaling) and image distortions (Noise addition, blurring, brightness change, color reduction and JPEG compression) get varied [2][3].

Manuscript published on 30 September 2019
* Correspondence Author
Dr.V.Thirunavukkarasu*, School of CSA, REVA University, Bengaluru, India
M.Ranganathappa, School of CSA, REVA University, Bengaluru, India
Dr.J.Satheesh Kumar, Department of Computer Applications, Bharathiar University, Coimbatore, India

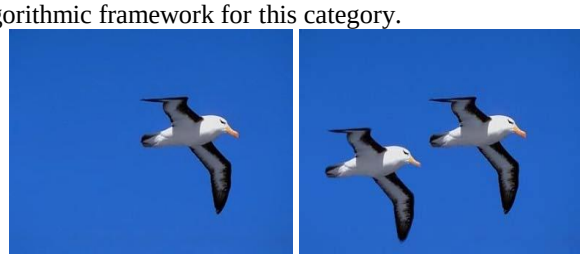
Organization of this article includes section II which introduces materials and methods in support of tamper finding. Section III depicts the empirical outcome on existing tamper detection methods. Section IV depicts the discussion and Challenges in Copy-Move tamper recognition. Conclusion of the manuscript is presented in section V,

II. MATERIALS AND METHODS

A. Algorithmic framework for Copy-move tamper detection

Discovering copy-move tampering requires profound analysis of local patterns or regions in an image.

One preliminary approach is to split the image of dimension M X N into different chunks (b X b) and comparing these chunks for similarity estimation. Dimension of the block will not exceed dimension of assumed tampered region. Each block of pixels are analyzed by means of four methods such as frequency transformation based method, dimensionality reduction method, moment and key point technique. Since the tampered image segments are in same image there exists a correlation between these two image segments. This kind of correlation can be detected with different feature matching and extensive search algorithms [4] [5]. Figure 1 exemplifies this type of manipulation and figure 2 illustrate the whole algorithmic framework for this category.



(a) (b)

Fig 1: (a) Authentic Image (b) Copy-Move Tampered image

B. Tamper exposure by means of Exhaustive search and Auto correlation

1) Exhaustive search

The elementary way to perceive copy-move tampering is to employ exhaustive search. The image has been shifted in to clockwise direction and shifted image has been compared with Original image as shown in figure 3. If P_{ij} is a pixel value of a gray scale image with dimension M X N at location (i, j), the subsequent disparity is calculated with exhaustive search,

$$\left|P_{ij} - P_{i+k\ mod(M)+l\ mod(N)}\right| \quad (1)$$

Where k=0, 1,……M-1, l=0,1,….N-1 designed for all i and j. Comparing P_{ij} by means of its clockwise shift [k,l] is similar to comparing P_{ij}

by its recurring shift [k' , l'] where k'=M-k and l'=N-l. Hence, it is sufficient to check merely clockwise shift [k,l] with 1≤k≤M/2, 1≤l≤N/2 . The technique is straightforward and successful for tiny scale images. Comparing segments with its cyclic shift leads high computational cost and not suitable for medium and large scale images [6].

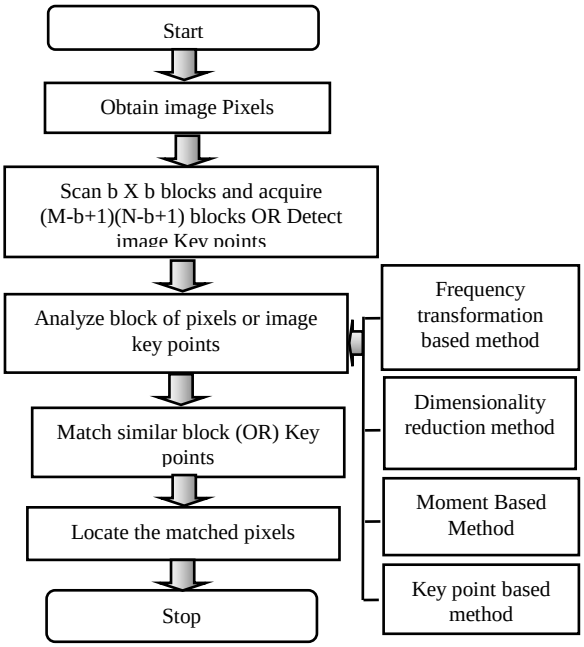


Fig 2: Algorithmic framework of Copy-move tampers detection

2) Autocorrelation method

Autocorrelation is another method to perceive copy-move tampering. It uses correlation among the original and pasted segments.

(a) (b)

Fig 3: (a) Authentic image (b) Image after shift

For images with M rows and N columns the correlation coefficients between image segments are computed using the formula,

$$AC(i,j) = \sum_{x=1}^{M}\sum_{y=1}^{N} \frac{f(x,y)f(x+i,y+j)}{MN} \qquad (2)$$

$AC(i,j)$ is the auto correlation function, f(x, y) indicates the significance of pixels at position (x,y). Variable i and j represent pixel lags. During the initial stage suspected region of the image is extracted and whole image is divided to number of sub-regions of size same as the extracted region. Autocorrelation function is performed among every sub-region of the image. Sub region having highest correlation is identified as tampered region. This method is a viable option for small scale images and not suitable for large scale images since, it has large computational overhead and often not succeeded to perceive the forgery [7]. Both Exhaustive and auto correlation methods are traditional methods having its own advantages and implementation issues.

III. RESULTS

Most of the methods reported in the literature encompass challenges like accuracy in tamper detection and false detection. In this section, three well known state of art methods such as frequency transformation based, PCA based and Zernike moment based methods are successfully implemented using MATLAB and experiments were carried out with three different bench mark data sets namely Kodak image dataset [8], CoMoFoD image data base [9] and Muhammad et al. dataset [10]. Detail descriptions of the above three data sets are presented in the table 1.

A. Data Set

1) KODAK image data set

The first bench mark KODAK image data set restrains 24 uncompressed true color images. All images are portable Network Graphic (PNG) format of size 768 X 512 pixels. Images regions are arbitrarily tampered with adobe Photoshop image editing tool.

Table 1: Description of three different dataset

Dataset	No. of Images			Image type	Image size
	Original	Tampered	Total		
KODAK	23	23	46	PNG	768 X 512
CoMoFoD	260	260	520	PNG	512 X 512
Muhammad et al.	10	10	20	JPEG	200 X 200

2) The CoMoFoD image data base

CoMoFoD data set comprise 260 authentic and 260 tampered images, out of those 200 images are under small category of size 512 X 512 pixels and 60 images are under big group of dimension 3000 X 2000 pixels. Different transformations are applied to tampered images and classified into five groups as follows,

1. Translation – The copied region is shifted into fresh position not including further transformations.
2. Rotation – tampered segment is spin with different angles also pasted in another location.
3. Scaling – tampered segment size is enlarged or diminished also pasted in another position.
4. Distortion – tampered province is deformed by various image distortions and interprets in to another position.
5. Combination – Copied region is deformed by two or more image transformations before it is moved to new location.

Different image distortions

Various image distortions performed on original and tampered images and their parameters are exposed in table 2.

Table 2: Parameters designed for diverse image distortion methods

Method	Parameter
JPEG compression	factor = [20, 30, 40, 50, 60, 70, 80, 90, 100]
Noise adding	μ = 0, σ2 = [0.009, 0.005, 0.0005]
Image blurring	filter = [3 X 3, 5 X 5, 7X 7]
Brightness change	[(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]
Colour reduction	Intensity levels per each colour channel =[32, 64, 128]
Contrast adjustments	[(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]

3) Muhammad et al. Data set

This data set includes numerous test images tampered with copy-move operation. There are 10 different source images and their tampered versions are created using Adobe Photoshop tool. Test images in this data set is not post processed and geometrically distorted.

4) Performance metrics

To reveal the accuracy of existing techniques, precision, recall and F metrics are employed. Precision exhibit the possibility of detected image is truly a forged image.

$$\text{Precision} = \frac{TP}{TP + FP} \qquad (3)$$

(3)

Where, true positive (TP) signifies the amount of tampered images correctly classified as tampered. False positive (FP) point out the number of original images classified as tampered. Recall is the possibility of forged image is perceived.

$$\text{Recall} = \frac{TP}{TP + FN} \qquad (4)$$

(4)

False negative FN designates the amount of tampered images classified as authentic. F coalesce precision and recall value while it is close [11]

$$F = 2 * \frac{P * R}{P + R} \qquad (5)$$

B. Frequency transformation based copy move tamper detection method

In this method, suspected input image is alienated into overlapping blocks and Discrete Cosine Transformation (DCT) coefficients are extracted from each overlapping blocks. Extracted coefficients are quantized with user specific parameter value Q for robust representation of image data and discover similar pattern in an image. Parameter value Q is indicate quality factor, the Q value is low false matches are high and the Q value is high false matches are low. Quantized DCT coefficients of each block are accumulated in single row matrixes A. The matrix restrain (M-b+1) (N-b+1) rows and b^2 columns where, M ,N signifies quantity of rows and columns and b signifies block size. If two consecutive rows of Quantized DCT coefficients are identical the algorithm stores position of matching block in a separate list and shift vector s is calculated with the formula,

$$s = (s1, s2) = (i1 - j1, i2 - j2) \qquad (6)$$

Where (i1, i2) and (j1, j2) indicates position matching blocks. The algorithm finds normalized shift vector whose incidence surpass user specific threshold (T). Value of T is related to size of smallest fragment. Detection result of this method is shown in figure 4[6].

C. Exposure of copy-move tampering with Principle Component Analysis (PCA)

PCA is a linear transformation technique in which the basic functions are obtained from statistical properties of image

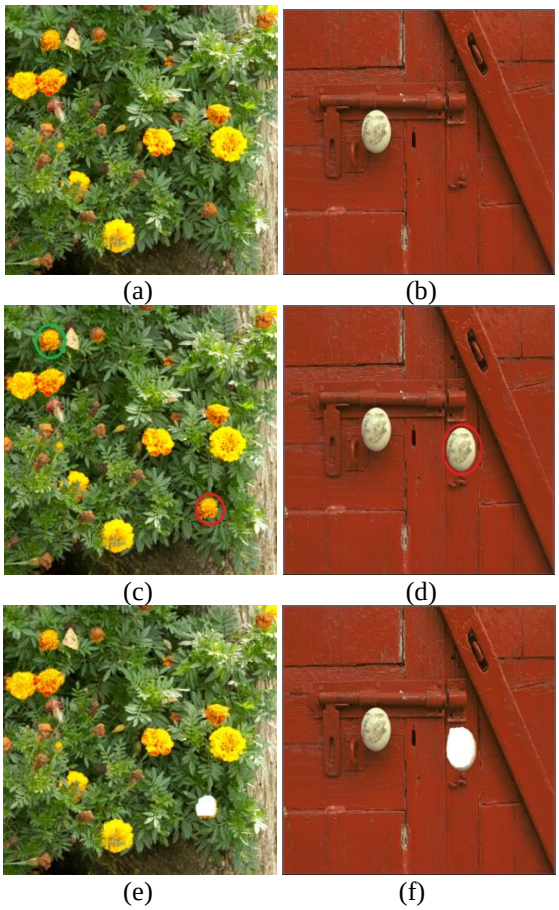


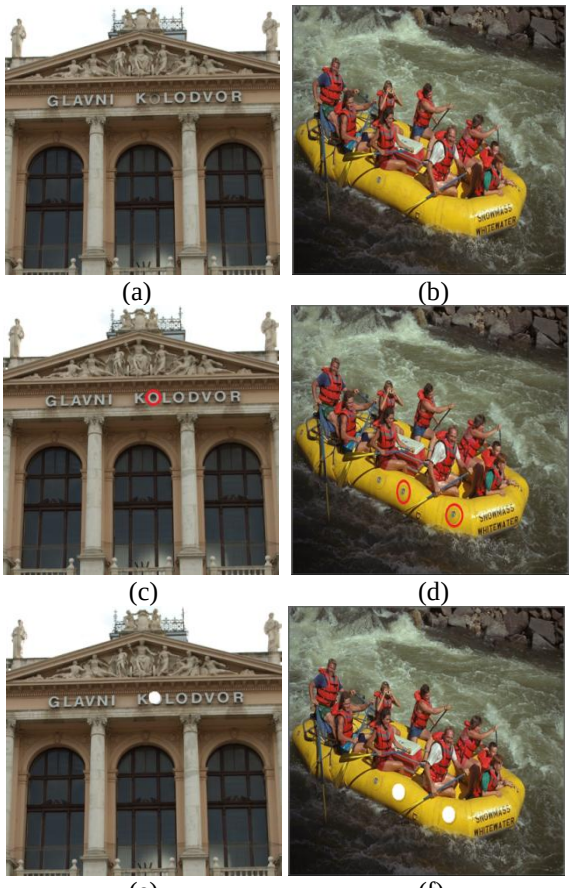
Fig 4: Frequency transform based copy-move tamper detection, (a) and (b) are authentic images, (c) and (d) are copy-move tampered images, (e) and (f) are detection results

data. It is optimal in the sense of energy compaction and well known method for reducing dimensionality of data. PCA renovate higher dimensional data into meaningful lower dimensional representation by means of Eigen vector decomposition of co-variance (or correlation) matrix. If data is projected on to eigenvector corresponding first largest Eigen value (Sometimes known as first principle component) then, it will reduce the data in to one dimension. If the data is projected on to Eigen vector corresponding to first and second largest Eigen value then, it will reduce the data into two dimensions. After reducing the dimension from d to k (k<d) the new set of coordinates are the linear combination of the original variables. First principle component has largest variance, second principle component has next largest variance and orthogonal to first one. This process will be continued until the dimension vector is reduced to k. When the dimension vector reached the maximum value all other variables are neglected without loss of information. Any square, symmetric, non-singular matrix can be transformed to a diagonal matrix using Eigen vectors.

PCA based technique is competent and stout practice to perceive copy move tampering. In this technique, the suspected gray scale image is alienated to small preset size blocks of B pixels and PCA is applied to all blocks to diminish the image dimension representation. Tampered regions are detected by matching similar PCA coefficients.
This method is used to identifies patterns in large set of data but infeasible for large size image blocks. Detection result of this method against simple and multiple copy-move tampering is shown in figure 5[12].

D. Zernike moment based tamper detection

Moments and its invariant properties are widely used in image registration, reconstruction and its related fields. Different types of moments are introduced in the literature. In this method, Seung et al. used Zernike moments to discover most common nature of counterfeit such as copy-move; it shows better result than other moments. In order to perceive the manipulation the suspected image f with dimension M X N is alienated into overlapping chunks of dimension



(a) (b) (c) (d) (e) (f)

Fig 5: Detection of copy-move tampering using PCA method, (a) and (b) are authentic images, (c) and (d) are copy-move tampered image, (e) and (f) are detection results.

L X L using the formula,

$$B_{ij}(x, y) = f(x + i, y + j) \quad (7)$$

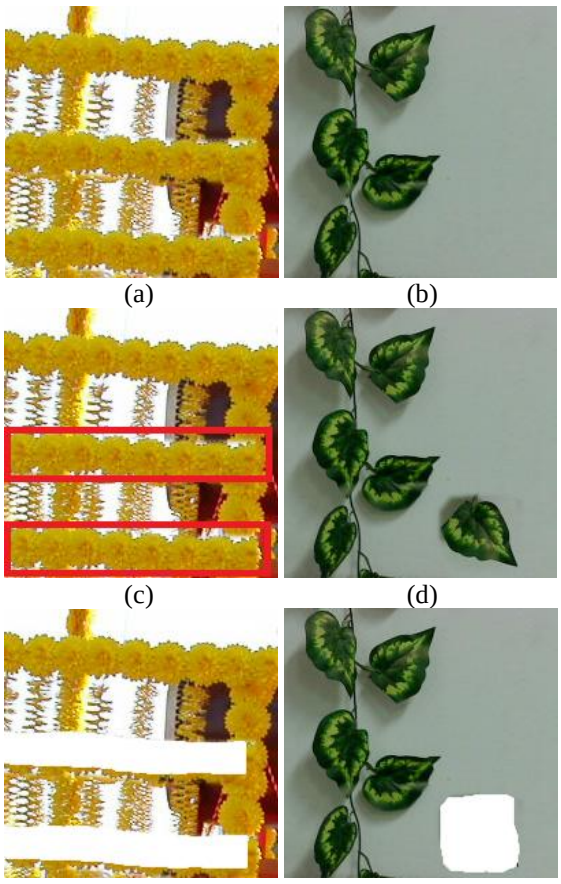
Where, x, yϵ {0.....L-1}, iϵ{0.....M-L}and jϵ{0.....N-L}and total number of blocks in the suspected input image is calculated with

$$N_{blocks}=(M-L+1)(N-L+1) \quad (8)$$

Zernike moments are extorted for every block B_{ij}, where i and j designate the initial points. Extracted Zernike moments are included in the two dimensional matrix and lexicographical sorting is applied. Analogous rows are closest to each other therefore Euclidean distance between two similar rows are calculated to match the tampered image. This method effectively detect simple, multiple tampering and rotated manipulation. Detection results are shown in figure 6[13].

IV. DISCUSSION

Experimental results demonstrate that the above three methods are efficient scheme to discover copy-move tampering. Performances of all three methods are evaluated under



(a) (b) (c) (d) (e) (f)

Fig 6: Revealing copy-move by means of Zernike method (a) and (b) are authentic images, (c) is multiple copy-move tampered image, (d) is tampered image rotated with clock wise 90 degree, (e) is the discovered result of (c), (f) is discovered outcome of (d).

simple copy-move tampering at image level. Overall performance comparison of these methods using different bench mark data base are shown in figure 7 to 9. The performance curve of PCA method out performs other two methods in all three dataset.
Computational complexity is yet another problem which is associated with block matching. Lexicographical matrix sorting is identified as a key factor related with computational difficulty.

Table 3 shows image representation and feature dimension of three methods. Out of three methods, Zernike method has reduced feature dimension but accuracy of the method is low over PCA method.

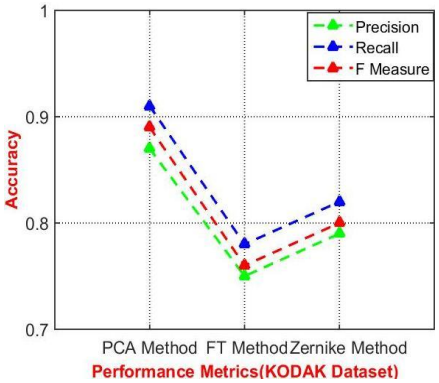


Fig 7: Comparison of experimental results with KODAK dataset

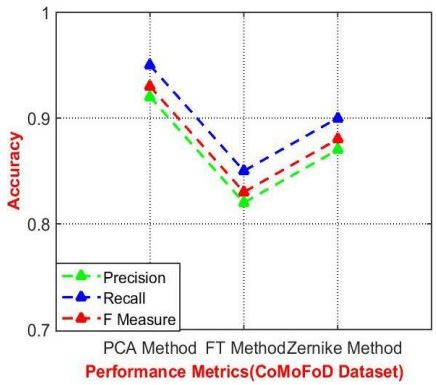


Fig 8: Comparison of experimental results with CoMoFoD dataset

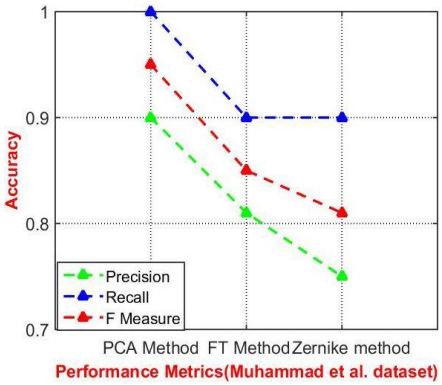


Fig 9: Comparison of experimental results with Muhammad et al. dataset

Table 3: Feature Dimension Comparison of different methods

Method	Image representation	Feature Dimension
Frequency transformation method	DCT	64
PCA method	PCA	32
Zernike method	Zernike moments	12

A. Challenges in Copy-Move tamper detection

Development of robust and efficient copy-move forgery detection techniques includes lot of challenges for researchers. This includes,

- ❖ Developing a distinctive as well as reliable method to perceive copy move tampering with different angel of rotation and various scaling factors.
- ❖ Detection of the forged region which is affected by illumination.
- ❖ Implementing detection system with dynamic view point change.
- ❖ Design of robust method to reduce false matches and improve the accuracy while perceive copy-move manipulation.
- ❖ Developing a method to distinguish the copy-move forgery in an image with dissimilar image deformation such as Blurring, brightness change, contrast adjustment, color reduction, noise addition and JPEG compression with different quality factor

V. CONCLUSION

This article focused the experimental analysis of three well known copy-move tamper detection techniques and its implementation issues. The general algorithmic framework and two traditional approaches in copy-move tamper detection are reviewed. From the existing methods, it is found that the reliable techniques need to be developed to identify the copy-move counterfeit when the image underwent some geometric transformation like translation, rotation and scaling. Apart from the transformation, the presence of forgery region and size of image will affect the performance of tamper detection method. Empirical result shows that a method having good accuracy rate may not have reduced features and vice versa. Hence, development of an optimized method for accurate tamper detection with reduced feature set will have higher influence in image based applications such as security and authentication.

ACKNOWLEDGEMNT

The authors would like to thank Vision Group of Science and Technology (VGST), Government of Karnataka, India for their financial support under the RGS/F grant (Grant No: KSTePS/VGST-RGS/F/GRD No.695/20L7).

REFERENCES

1. Gajanan K Birajdar, Vijay H Mankar, “Digital image forgery detection using passive techniques: A survey”,. Digital Investigation, 2013; 10 (1): 226–245.
2. Thirunavukkarasu V, Satheesh Kumar J, “Evolution of blind methods for image tamper detection-A review”, International Journal of Applied Engineering Research, 2014; 9 (21): 5069–76.
3. Thirunavukkarsu V, Satheesh Kumar J, “A novel method to detect copy-move tampering in digital images”, IND-JST, 2016; 9(8):1–4.
4. V.Thirunavukkarasu, J.Satheeshkumar, “Passive Image Tamper Detection Technique Based on Moment Invariants”, IJCTA.2016;.9 (10): 4705-4714.
5. V. Thirunavukkarasu, J Satheesh Kumar, Gyoo Soo Chae, J. Kishorkumar, “Non-intrusive Forensic Detection Method Using DSWT with Reduced Feature Set for Copy-Move ImageTampering”, Wireless Personal Communications. 2017; .98(1): 3039–3057.
6. Fridrich A, Jessica B, David Soukal, A. Jan Lukas, “Detection of copy-move forgery in digital images”,. In Proceedings of Digital Forensic Research Workshop, 2003.
7. A. C. Popescu, H. Farid, “Statistical tools for digital forensics. Information Hiding”, 2004; 32(1): 395-407.

8. Kodak Lossless True Color Image Suite: http://r0k.us/graphics/kodak/
9. Tralic D, Zupancic I, Grgic S, Grgic M. CoMoFoD - New Database for Copy-Move Forgery Detection. In Proc. 55th International Symposium ELMAR.2013. 49-54.
10. Muhammad G, Hussain M, Khawaji K, Bebis G, "Blind copy move image forgery detection using dyadic un-decimated wavelet transform",. Digital signal processing.2011:1-6.
11. V.Thirunavukkarasu, J.Satheeshkumar, "Passive Image Tamper Detection Based on Fast Retina Key point Descriptor", IEEE-ICACA. 2016; 279-285.
12. A. Popescu, H. Farid., "Exposing digital forgeries by detecting duplicated image regions", Technical Report TR2004-515. 2004: Department of Computer Science, Dartmouth College.
13. Ryu, Seung-Jin, Min-Jeong Lee, Heung-Kyu Lee, "Detection of copy-rotate-move forgery using zernike moments", Information Hiding. 2010; 638(7):51-65.

AUTHORS PROFILE

Dr.V.Thirunavukkarasu, received his doctoral degree in computer science from Bharathiar University, Tamil Nadu, India. Currently he is working as an Assistant Professor, School of Computer science and Applications, REVA University, Bengaluru, India. His area of interest includes image forensic investigation, computational intelligence and machine learning algorithms. (E-mail: arasu_mca3@yahoo.com)

M.Ranganathappa, received his master degree in computer science and applications from Sri Venkateswara University, Tirupathi, Andhra Pradesh, India. Currently he is working as an Assistant Professor, School of Computer science and Applications, REVA University, Bengaluru, India. He is having 10 plus years of teaching experience. His area of interest includes Image processing and data mining. (E-mail: rangegowda18@gmail.com)

Dr. J. Satheesh Kumar is with the Department of Computer Applications, School of Computer Science and Engineering, Bharathiar University, Coimbatore, Tamil Nadu, India. He is having 16 plus years of research and teaching experience. His area of specialization includes soft computing, networks, Image processing and medical imaging.(E-mail: jsathee@rediffmail.com)